UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,797	01/09/2006	Naoki Yamamoto	2005_1975A	5364

513 7590 08/27/2008

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
POGMORE, TRAVIS D	
ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
08/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/563,797	YAMAMOTO ET AL.	
	Examiner	Art Unit	
	TRAVIS POGMORE	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☒ Claim(s) *1 and 6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09 January 2006, 27 February 2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/563,797 filed on January 9, 2006 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in 37 C.F.R. 1.63.

Priority

3. As required by M.P.E.P. 201.14(c), acknowledgement is made of applicant's claim for priority based on applications filed on August 5, 2003.

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

5. As required by M.P.E.P. 609, the applicant's submissions of the Information Disclosure Statements dated January 9, 2006 and February 27, 2006 is acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending Japanese Patent Application Pub. No. 2000-023137 (Masuda et al.) and 08-181689 (Kubota et al.) were not considered because they are the same inventions as U.S. Patent No. 6,714,649 and 5,721,778 respectively which are also cited in the January 9th IDS.

Drawings

6. The applicant's drawings submitted are acceptable for examination purposes.

Claim Objections

7. Claim 1 is objected to because of the following informalities: It is not the least restrictive claim presented as it consists of all limitations recited in claims 7, 13 and 19. See 37 CFR 1.75.

8. Claim 6 is objected to because of the following informalities: In line 2 it recites "said recording apparatuses". There is insufficient antecedent basis for this limitation in the claim as only a single recording apparatus was previously recited. For the purposes of this examination it will be assumed that this instance of "recording apparatuses" in the claim should be replaced with "reproduction apparatuses".

In line 3 the claim recites "second reproduction apparatus" and "second category". There is insufficient antecedent basis for this limitation in the claim as neither "first reproduction apparatus" nor "first category" was previously recited. Appropriate correction is required.

Claim Rejections – 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 33 and 34 are rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. The claims lack the necessary physical articles or

objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

Claim Rejections – 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1-2, 6-8, 12-14, 18-20, and 24-34 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6,118,873 (hereinafter “Lotspiech et al.”).

As to claim 1, Lotspiech et al. teaches a copyright protection system comprising: a recording apparatus operable to encrypt a content and to record the encrypted content (Fig. 1, elements 12 and 14, 12 being the recording apparatus and 14 an encryption module); a recording medium on which the encrypted content is recorded (column 10, lines 35-41, in particular it recites DVD movies); and reproduction apparatuses, each of which is operable to read out and decrypt the encrypted content recorded on said recording medium (column 1, line 67 to column 2 line 2 and column 2, lines 10-17, the “plural user devices” being the reproduction apparatuses),

wherein said reproduction apparatuses are classified into N-categories, N being a natural number greater than one (column 2, lines 18-27 and column 5, lines 34-41, where the M sets dimension are the N-categories),

said recording apparatus is operable (a) to generate, for the respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key (Abstract, lines 9-14 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories and any “dummy number(s)” along with the other valid session numbers are the revocation data), (b) to generate the encrypted content which is the content encrypted based on

the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and (c) to record at least the N-pieces of revocation data and the encrypted content onto said recording medium (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”), the device key data being held by said reproduction apparatuses of the respective N-categories (column 2, lines 10-13), and the device key being held by a specific reproduction apparatus of the respective categories (column 5, lines 50-54), and

said reproduction apparatuses are each operable (a) to read out, from said recording medium, revocation data (column 2, lines 10-17, as recited the session keys (including any “dummy numbers”) are the revocation data), among the N-pieces of revocation data, which is for the category to which said reproduction apparatus belongs, and the encrypted content (column 2, lines 10-13), and (b) to decrypt the encrypted content based on the read-out revocation data (column 2, lines 13-17).

As to claim 2, Lotspiech et al. teaches wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatuses of a corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces), and

said reproduction apparatuses of the respective categories are each operable (a) to read out, from said recording medium, the corresponding encrypted media key data and the encrypted content (column 2, lines 10-13 and column 2, lines 10-17, as recited the session keys (including any “dummy numbers”) are the revocation data), (b) to obtain the media key by decrypting the encrypted media key data using the held device key (column 2, lines 30-38), and (c) to decrypt the encrypted content based on the obtained media key (column 2, lines 13-17).

As to claim 6, Lotspiech et al. teaches wherein said recording apparatuses are made up of:

second reproduction apparatuses belonging to a second category (column 2, lines 18-27 and column 5, lines 50-54, where the M sets dimension are the N-categories, it is inherent that given at least 2 reproduction apparatuses with unique device keys that at least one of them must belong to a second category, else they would not actually be unique device keys), each of which is operable to read out and decrypt the encrypted content recorded on the recording medium; and

first reproduction apparatuses (column 2, lines 18-27 and column 5, lines 50-54, as above given 2 reproduction apparatuses with unique device keys and one in a second category, the other one must be in a first category), each of which includes: a read-out apparatus of the second category operable to read out and perform a part of a decryption process on the encrypted content recorded on the recording medium (column 1, lines 30-38, e.g. a DVD player in combination with a set-top box); and

a decryption apparatus of a first category, connected to said read-out apparatus of the second category, operable to perform a part of the decryption process on the encrypted content (column 1, lines 30-38, e.g. a digital television),

wherein said recording apparatus is operable (a) to generate, based on a media key and on device key data held by said decryption apparatuses of the first category, first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) to generate, based on a media key and on device key data held by said apparatuses of the second category, second revocation data intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and any “dummy number(s)” along with the other valid session numbers are the revocation data), (c) to generate an encrypted content which is the content encrypted based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and (d) to record at least the first revocation data, the second revocation data, and the encrypted content onto said recording medium (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”),

said second reproduction apparatuses are each operable to read out the second revocation data and the encrypted content from said recording medium (column 2, lines

10-13), and to decrypt the encrypted content based on the second revocation data (column 2, lines 13-17), and

in each of said first reproduction apparatuses:

said read-out apparatus of the second category is operable (a) to read out, from said recording medium, the first revocation data, the second revocation data, and the encrypted content (column 2, lines 10-13), and (to) supply intermediate data and the first revocation data to said decryption apparatus of the first category (column 2, lines 13-17 and column 9, lines 38-49, the set-top box receives the broadcast from the DVD player, any session-key block (which includes the second revocation data) is passed through the set-top box and the content is re-encrypted to allow only legitimate devices to view or record it); and

said decryption apparatus of the first category is operable to obtain the content by performing the decryption process, based on the first revocation data, on the intermediate data supplied by said read-out apparatus of the second category, the intermediate data being the encrypted data on which the part of the decryption process has been performed based on the second revocation data (column 9, lines 44-46).

As to claim 7, Lotspiech et al. teaches a recording apparatus which encrypts a content and records the encrypted content (Fig. 1, elements 12 and 14, 12 being the recording apparatus and 14 an encryption module),

wherein said recording apparatus is operable (a) to generate, for respective N-categories and based on a media key and device key data, revocation data intended for

revoking a device key (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories and any “dummy number(s)” along with the other valid session numbers are the revocation data), (b) to generate an encrypted content which is the content encrypted based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and (c) to record at least the N-pieces of revocation data and the encrypted content onto a recording medium (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”), the device key data being held by reproduction apparatuses classified into N-categories and belonging to the respective categories (column 2, lines 10-13), the device key being held by a specific reproduction apparatus of the respective categories, and N being a natural number greater than one (column 5, lines 34-41 and 50-54).

As to claim 8, Lotspiech et al. teaches wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by the reproduction apparatuses of a corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces).

As to claim 12, Lotspiech et al. teaches wherein said recording apparatus (a) generates, based on a media key and on device key data held by decryption apparatuses of the first category, first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) generates, based on a media key and on device key data held by apparatuses of the second category, second revocation data intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and any “dummy number(s)” along with the other valid session numbers are the revocation data), and (c) generates an encrypted content which is the content encrypted based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and to record at least the first revocation data, the second revocation data, and the encrypted content onto the recording medium (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”).

As to claim 13, Lotspiech et al. teaches a recording medium on which a content is recorded (column 10, lines 35-41, in particular it recites DVD movies),

wherein on said recording medium, at least revocation data and an encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast"

the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the revocation data being generated based on a media key and device key data and intended for revoking a device key (Abstract, lines 9-18), the device key data being held by reproduction apparatuses classified into N-categories and belonging to the respective categories (column 2, lines 10-13), the device key being held by a specific reproduction apparatus of the respective categories (column 5, lines 50-54), the encrypted content being generated by encrypting the content based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and N being a natural number greater than one (column 5, lines 34-41 and 50-54).

As to claim 14, Lotspiech et al. teaches wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatuses of a corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces).

As to claim 18, Lotspiech et al. teaches wherein on said recording medium, at least first revocation data, second revocation data, and the encrypted content are

recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the first revocation data being generated based on the media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and any “dummy number(s)” along with the other valid session numbers are the revocation data), and the encrypted content being the content on which an encryption process has been performed based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption).

As to claim 19, Lotspiech et al. teaches a reproduction apparatus which reproduces an encrypted content recorded on a recording medium (column 1, line 67 to column 2 line 2 and column 2, lines 10-17, the “plural user devices” being the reproduction apparatuses),

wherein said reproduction apparatuses are classified into N-categories, N being a natural number greater than one (column 2, lines 18-27 and column 5, lines 34-41, where the M sets dimension are the N-categories),

on the recording medium, at least revocation data and an encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the revocation data being generated based on a media key and device key data and intended for revoking a device key (Abstract, lines 9-18), the device key data being held by said reproduction apparatuses of the respective N-categories (column 2, lines 10-13), the device key being held by a specific reproduction apparatus of the respective categories (column 5, lines 50-54), and the encrypted content being generated by encrypting the content based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and

said reproduction apparatus is operable (a) to read out, from the recording medium, revocation data, among the N-pieces of revocation data, which is for the category to which said reproduction apparatus belongs, and the encrypted content (column 2, lines 10-13), and (b) to decrypt the encrypted content based on the read-out revocation data (column 2, lines 13-17).

As to claim 20, Lotspiech et al. teaches wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatuses of a corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces), and

said reproduction apparatuses are operable (a) to read out, from the recording medium, the corresponding encrypted media key data and the encrypted content (column 2, lines 10-13 and column 2, lines 10-17, as recited the session keys (including any “dummy numbers”) are the revocation data), (b) to obtain the media key by decrypting the encrypted media key data using the held device key (column 2, lines 30-38), and (c) to decrypt the encrypted content based on the obtained media key (column 2, lines 13-17).

As to claim 24, Lotspiech et al. teaches wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the first revocation data being generated based on the media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data

being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and any “dummy number(s)” along with the other valid session numbers are the revocation data), and the encrypted content being the content on which an encryption process has been performed based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and

said reproduction apparatus belongs to the second category (column 2, lines 18-27 and column 5, lines 50-54, where the M sets dimension are the N-categories, it is inherent that given at least 2 reproduction apparatuses with unique device keys that at least one of them must belong to a second category, else they would not actually be unique device keys) and is operable to read out, from the recording medium, the second revocation data and the encrypted content (column 2, lines 10-13), and to decrypt the encrypted content based on the second revocation data (column 2, lines 13-17).

As to claim 25, Lotspiech et al. teaches a read-out apparatus included in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium (column 1, lines 30-38, e.g. a DVD player in combination with a set-top box),

wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the first revocation data being generated based on a media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and any “dummy number(s)” along with the other valid session numbers are the revocation data), and the encrypted content being the content on which an encryption process has been performed based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and

said read-out apparatus belongs to the second category and is operable (a) to read out, from the recording medium, the first revocation data, the second revocation data, and the encrypted content (column 2, lines 10-13), (b) to generate intermediate data which is the encrypted data on which a part of a decryption process has been

performed, based on the second revocation data (column 2, lines 13-17), and (c) to output the generated intermediate data and the first revocation data (column 9, lines 38-49, the set-top box receives the broadcast from the DVD player, any session-key block (which includes the second revocation data) is passed through the set-top box and the content is re-encrypted to allow only legitimate devices to view or record it).

As to claim 26, Lotspiech et al. teaches a decryption apparatus included in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium (column 1, lines 30-38, e.g. a digital television),

wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the first revocation data being generated based on a media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and

any “dummy number(s)” along with the other valid session numbers are the revocation data), and the encrypted content being the content on which an encryption process has been performed based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and

read-out apparatuses of the second category are each operable (a) to read out, from the recording medium, the first revocation data, the second revocation data, and the encrypted content (column 2, lines 10-13), (b) to generate intermediate data which is the encrypted data on which a part of a decryption process has been performed, based on the second revocation data (column 2, lines 13-17), and (c) to output the generated intermediate data and the first revocation data (column 9, lines 38-49, the set-top box receives the broadcast from the DVD player, any session-key block (which includes the second revocation data) is passed through the set-top box and the content is re-encrypted to allow only legitimate devices to view or record it), and

said decryption apparatus belongs to the first category and is operable to obtain the content by performing a decryption process, based on the first revocation data, on the intermediate data supplied by said read-out apparatus of the second category (column 9, lines 44-46).

As to claim 27, Lotspiech et al. teaches a reproduction apparatus which reproduces an encrypted content recorded on a recording medium, said reproduction

apparatus comprising: said read-out apparatus according to claim 25; and a decryption apparatus which reproduces an encrypted content recorded on a recording medium,

wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the first revocation data being generated based on a media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories including the first and second specific apparatuses and any “dummy number(s)” along with the other valid session numbers are the revocation data), and the encrypted content being the content on which an encryption process has been performed based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and

read-out apparatuses of the second category are each operable (a) to read out, from the recording medium, the first revocation data, the second revocation data, and

the encrypted content (column 2, lines 10-13), (b) to generate intermediate data which is the encrypted data on which a part of a decryption process has been performed, based on the second revocation data (column 2, lines 13-17), and (c) to output the generated intermediate data and the first revocation data (column 9, lines 38-49, the set-top box receives the broadcast from the DVD player, any session-key block (which includes the second revocation data) is passed through the set-top box and the content is re-encrypted to allow only legitimate devices to view or record it), and

said decryption apparatus belongs to the first category and is operable to obtain the content by performing a decryption process, based on the first revocation data, on the intermediate data supplied by said read-out apparatus of the second category (column 9, lines 44-46).

As to claim 28, Lotspiech et al. teaches a copyright protection system comprising:

a key generation apparatus operable to generate and record revocation data necessary for encrypting and decrypting a content (Fig. 1, elements 12 and 14, 12 being the recording apparatus and 14 an encryption module),

recording apparatuses, each of which is operable to encrypt a content and to record the encrypted content (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”);

a recording medium on which the encrypted content and the revocation data are recorded (column 10, lines 35-41, in particular it recites DVD movies); and

reproduction apparatuses, each of which is operable to read out and decrypt the encrypted content recorded on said recording medium (column 1, line 67 to column 2 line 2 and column 2, lines 10-17, the “plural user devices” being the reproduction apparatuses),

wherein said recording apparatuses and said reproduction apparatuses are classified into N-categories, N being a natural number greater than one (column 2, lines 18-27 and column 5, lines 34-41, where the M sets dimension are the N-categories),

said key generation apparatus is operable (a) to generate, for the respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories and any “dummy number(s)” along with the other valid session numbers are the revocation data), and (b) to record the N-pieces of revocation data onto said recording medium (Fig. 6, element 52, as recited the “session key block”), the device key data being held by one of said recording apparatuses and said reproduction apparatuses belonging to the respective N-categories (column 2, lines 18-27 and column 5, lines 50-54, where the M sets dimension are the N-categories), the device key being held by one of a specific recording apparatus and a specific reproduction apparatus of the respective categories (column 5, lines 50-54),

said recording apparatuses are each operable (a) to read out, from said recording medium, revocation data among the N-pieces of revocation data, which is for

the category to which said recording apparatus belongs (column 9, lines 38-44), (b) to generate the encrypted content by encrypting the content based on the read-out revocation data (column 9, lines 44-46), and (c) to record the generated encrypted content on said recording medium (column 9, lines 36-40 and 44-46, it is inherent that a device such as a VCR which generates encrypted data and then allows other devices to decrypt it must be able to record said encrypted data at some point), and

said reproduction apparatuses are each operable (a) to read out, from said recording medium, revocation data (column 2, lines 10-17, as recited the session keys (including any “dummy numbers”) are the revocation data), among the N-pieces of revocation data, which is for the category to which said reproduction apparatus belongs, and the encrypted content (column 2, lines 10-13), and (b) to decrypt the encrypted content based on the read-out revocation data (column 2, lines 13-17).

As to claim 29, Lotspiech et al. teaches a key generation apparatus which generates (Fig. 1, elements 12 and 14, 12 being the recording apparatus and 14 an encryption module), for respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories and any “dummy number(s)” along with the other valid session numbers are the revocation data), and which records the generated N-pieces of revocation data onto a recording medium (Fig. 6, element 52, as recited the “session

key block"), the device key data being held by one of the recording apparatuses and the reproduction apparatuses classified into N-categories and belonging to the respective categories (column 2, lines 18-27 and column 5, lines 50-54, where the M sets dimension are the N-categories), the device key being held by one of a specific recording apparatus and a specific reproduction apparatus of the respective categories, and N being a natural number greater than one (column 5, lines 34-41 and 50-54).

As to claim 30, Lotspiech et al. teaches a recording apparatus which encrypts a content and records the encrypted content (column 9, lines 34-49),

wherein said recording apparatus is operable (a) to read out, from a recording medium on which N-pieces of revocation data are recorded, revocation data for a category to which said recording apparatus belongs (column 9, lines 38-44), (b) to generate an encrypted content by encrypting the content based on the read-out revocation data (column 9, lines 44-46), and (c) to record the generated encrypted content onto the recording medium (column 9, lines 36-40 and 44-46, it is inherent that a device such as a VCR which generates encrypted data and then allows other devices to decrypt it must be able to record said encrypted data at some point), the revocation data being generated based on a media key and device key data and intended for revoking a device key (Abstract, lines 9-18), the device key data being held by one of recording apparatuses and reproduction apparatuses which are classified into N-categories and belonging to the respective categories (column 2, lines 10-13), the device key being held by one of a specific recording apparatus and a specific

reproduction apparatus of the respective categories, and N being a natural number greater than one (column 5, lines 34-41 and 50-54).

As to claim 31, Lotspiech et al. teaches a recording method for use in a recording apparatus which encrypts a content and records the encrypted content (the recording apparatus described in claim 7 recites the particular steps of this method in this particular order), said method comprising:

a step of generating, for respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories and any “dummy number(s)” along with the other valid session numbers are the revocation data), the device key data being held by the reproduction apparatuses classified into the N-categories (column 2, lines 10-13) and belonging to the respective N-categories, the device key being held by a specific reproduction apparatus of the respective categories, and N being a natural number greater than one (column 5, lines 34-41 and 50-54);

an encrypted content generation step of generating the encrypted content by encrypting the content, based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption); and

a recording step of recording at least the N-pieces of revocation data and the encrypted content onto the recording medium (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”).

As to claim 32, Lotspiech et al. teaches a reproduction method for use in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium (the reproduction apparatus described in claim 19 recites the particular steps of this method in this particular order),

wherein the reproduction apparatuses are classified into N-categories, N being a natural number greater than one (column 2, lines 18-27 and column 5, lines 34-41, where the M sets dimension are the N-categories),

on the recording medium, at least revocation data and the encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the revocation data being generated based on a media key and device key data and intended for revoking a device key (Abstract, lines 9-18), the device key data being held by the reproduction apparatuses of the respective N-categories (column 5, lines 34-41 and 50-54), the device key being held by a specific reproduction apparatus of the respective categories (column 5, lines 50-54), and the encrypted content being generated by encrypting the content based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is

inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption), and

said reproduction method comprises:

a read-out step of reading out, from the recording medium: revocation data among the N-pieces of revocation data, for the category to which the reproduction apparatus belongs; and the encrypted content (column 2, lines 10-13);

and a decryption step of decrypting the encrypted content based on the revocation data read out in said read-out step (column 2, lines 13-17).

As to claim 33, Lotspiech et al. teaches a program for use in a recording apparatus which encrypts a content and records the encrypted content (the recording method described in claim 31 recites the particular steps of this program in this particular order), said program comprising:

a step of generating, for respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-categories and any “dummy number(s)” along with the other valid session numbers are the revocation data), the device key data being held by the reproduction apparatuses classified into the N-categories (column 2, lines 10-13) and belonging to the respective N-categories, the device key being held by a specific

reproduction apparatus of the respective categories, and N being a natural number greater than one (column 5, lines 34-41 and 50-54);

an encrypted content generation step of generating the encrypted content by encrypting the content, based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a “common key” as recited must be used for encryption as well as the explicitly stated decryption); and

a recording step of recording at least the N-pieces of revocation data and the encrypted content onto the recording medium (Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”).

As to claim 34, Lotspiech et al. teaches a program for use in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium (the reproduction method described in claim 32 recites the particular steps of this program in this particular order),

wherein the reproduction apparatuses are classified into N-categories, N being a natural number greater than one (column 2, lines 18-27 and column 5, lines 34-41, where the M sets dimension are the N-categories),

on the recording medium, at least revocation data and the encrypted content are recorded (column 10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and encrypted content in the form of a DVD movie as suggested it must be on a recording medium, in particular a DVD), the revocation data being generated based on a media key and device key data and intended for revoking a

device key (Abstract, lines 9-18), the device key data being held by the reproduction apparatuses of the respective N-categories (column 5, lines 34-41 and 50-54), the device key being held by a specific reproduction apparatus of the respective categories (column 5, 50-54), and the encrypted content being generated by encrypting the content based on the media key (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as recited must be used for encryption as well as the explicitly stated decryption), and

said reproduction program comprises:

a read-out step of reading out, from the recording medium: revocation data among the N-pieces of revocation data, for the category to which the reproduction apparatus belongs; and the encrypted content (column 2, lines 10-13);

and a decryption step of decrypting the encrypted content based on the revocation data read out in said read-out step (column 2, lines 13-17).

Claim Rejections – 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 3, 9, 15, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al. in view of U.S. Patent Application Pub. No. US 2001/044897 A1 (hereinafter "Ishiguro et al.").

As to claim 3, Lotspiech et al. teaches the copyright protection system as recited in claim 2, but does not specifically teach wherein said recording apparatus is operable to generate an encryption key based on the media key, and to encrypt the content based on the encryption key, and said reproduction apparatuses of the respective categories are each operable to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

However Ishiguro et al. teaches wherein said recording apparatus is operable to generate an encryption key based on the media key, and to encrypt the content based on the encryption key (page 5, paragraph 73, lines 5-8 and 11-14), and said reproduction apparatuses of the respective categories are each operable to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key (page 5, paragraph 73, lines 8-11 and 14-16).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt the content using an additional key as in Ishiguro et al. because it provides an additional layer of security.

As to claim 9, Lotspiech et al. teaches the recording apparatus according to claim 8, but does not specifically teach wherein said recording apparatus generates an

encryption key based on the media key, and to encrypt the content based on the encryption key.

However Ishiguro et al. teaches wherein said recording apparatus generates an encryption key based on the media key, and to encrypt the content based on the encryption key (page 5, paragraph 73, lines 5-8 and 11-14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt the content using an additional key as in Ishiguro et al. because it provides an additional layer of security.

As to claim 15, Lotspiech et al. teaches the recording medium according to claim 14, but does not specifically teach wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key.

However Ishiguro et al. teaches wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key (page 5, paragraph 73, 11-14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt the content using an additional key as in Ishiguro et al. because it provides an additional layer of security.

As to claim 21, Lotspiech et al. teaches the reproduction apparatus according to claim 20, but does not specifically teach wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key, and said reproduction apparatus is operable to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

However Ishiguro et al. teaches wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key (page 5, paragraph 73, 11-14), and said reproduction apparatus is operable to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key (page 5, paragraph 73, lines 8-11 and 14-16).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt and decrypt the content using an additional key as in Ishiguro et al. because it provides an additional layer of security.

15. Claims 4-5, 10-11, 16-17, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al. in view of European Patent Application Pub. No. EP 0969667 A2 (hereinafter “Masuda et al.”).

As to claim 4, Lotspiech et al. teaches the copyright protection system as recited in claim 2, but does not specifically teach wherein said recording apparatus is operable to encrypt the content using a content key, to generate an encrypted content key by encrypting the content key using the media key, and to record the generated encrypted content key onto said recording medium, and said reproduction apparatuses of the respective categories are each operable to read out the encrypted content key from said recording medium, to obtain the content key by decrypting the encrypted content key using the media key, and to decrypt the encrypted content using the obtained content key.

However Masuda et al. teaches wherein said recording apparatus is operable to encrypt the content using a content key (page 2, lines 49-50, the "scramble key"), to generate an encrypted content key by encrypting the content key using the media key (page 2, lines 53-56 and page 3, line 11, where the “second key” is the media key), and to record the generated encrypted content key onto said recording medium (page 2, lines 56-58), and said reproduction apparatuses of the respective categories are each operable to read out the encrypted content key from said recording medium (page 2, line 58 to page 3, line 2), to obtain the content key by decrypting the encrypted content key using the media key (page 3, lines 3-5), and to decrypt the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt the content

using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 5, Lotspiech et al. teaches the copyright protection system as recited in claim 1,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by said reproduction apparatuses of the corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces), but does not specifically teach wherein

said recording apparatus is operable to encrypt the content using a content key, to generate N-pieces of encrypted content keys by encrypting the content key using N-pieces of media keys, and to record, onto said recording medium, at least the N-pieces of encrypted media key data, the N-pieces of encrypted content keys, and the encrypted content, and

said reproduction apparatuses of the respective categories are each operable (a) to read out, from said recording medium, the encrypted media key data for the corresponding category, the encrypted content key for the corresponding category, and the encrypted content, (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key, (c) to obtain the content key by decrypting the encrypted content key for the corresponding category

using the obtained media key for the corresponding category, and (d) to decrypt the encrypted content using the obtained content key.

However Masuda et al. teaches wherein said recording apparatus is operable to encrypt the content using a content key (page 2, lines 49-50, the "scramble key"), to generate N-pieces of encrypted content keys by encrypting the content key using N-pieces of media keys (page 2, lines 53-56 and page 3, line 11, where the “second key” is the session key block (i.e. media key) as recited in Lotspiech et al.), and to record, onto said recording medium, at least the N-pieces of encrypted media key data (Lotspiech et al., Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”), the N-pieces of encrypted content keys, and the encrypted content (page 2, lines 56-58), and

said reproduction apparatuses of the respective categories are each operable (a) to read out, from said recording medium, the encrypted media key data for the corresponding category, the encrypted content key for the corresponding category, and the encrypted content (page 2, line 58 to page 3, line 2), (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key (Lotspiech et al., column 2, lines 30-38), (c) to obtain the content key by decrypting the encrypted content key for the corresponding category using the obtained media key for the corresponding category (page 3, lines 3-5), and (d) to decrypt the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt and decrypt the

content using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 10, Lotspiech et al. teaches the recording apparatus according to claim 8, but does not specifically teach wherein said recording apparatus encrypts the content using a content key, generates an encrypted content key which is the content key encrypted using the media key, and records the generated encrypted key onto the recording medium.

However Masuda et al. teaches wherein said recording apparatus encrypts the content using a content key (page 2, lines 49-50, the "scramble key"), generates an encrypted content key which is the content key encrypted using the media key (page 2, lines 53-56 and page 3, line 11, where the “second key” is the media key), and records the generated encrypted key onto the recording medium (page 2, lines 56-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt the content using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 11, Lotspiech et al. teaches the recording apparatus according to claim 7,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data

held by said reproduction apparatuses of the corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces), but does not specifically teach wherein

said recording apparatus is operable (a) to encrypt the content using a content key, (b) to generate N-pieces of encrypted content keys by encrypting the content key using N-pieces of media keys, and (c) to record, onto the recording medium, at least the N-pieces of encrypted media key data, the N-pieces of encrypted content keys, and the encrypted content.

However Masuda et al. teaches wherein said recording apparatus is operable (a) to encrypt the content using a content key (page 2, lines 49-50, the "scramble key"), (b) to generate N-pieces of encrypted content keys by encrypting the content key using N-pieces of media keys (page 2, lines 53-56 and page 3, line 11, where the “second key” is the session key block (i.e. media key) as recited in Lotspiech et al.), and (c) to record, onto the recording medium, at least the N-pieces of encrypted media key data (Lotspiech et al., Fig. 6, elements 52 and 54, as recited the “session key block” and the “encrypted program”), the N-pieces of encrypted content keys, and the encrypted content (page 2, lines 56-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt and decrypt the content using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 16, Lotspiech et al. teaches the recording medium according to claim 14, but does not specifically teach wherein the encrypted content is generated by encrypting the content using a content key, and on said recording medium, an encrypted content key is recorded, the encrypted content key being generated by encrypting the content key using the media key.

However Masuda et al. teaches wherein the encrypted content is generated by encrypting the content using a content key (page 2, lines 49-50, the "scramble key"), and on said recording medium, an encrypted content key is recorded (page 2, lines 56-58), the encrypted content key being generated by encrypting the content key using the media key (page 2, lines 53-56 and page 3, line 11, where the “second key” is the media key).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt the content using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 17, Lotspiech et al. teaches the recording medium according to claim 13,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by the reproduction apparatuses of the corresponding category (column 2, lines 2-

10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces), but does not specifically teach wherein

the encrypted content is generated by encrypting the content using a content key, or

on said recording medium, N-pieces of encrypted content keys generated by encrypting the content key using the N-pieces of media keys are recorded.

However Masuda et al. teaches wherein the encrypted content is generated by encrypting the content using a content key (page 2, lines 49-50, the "scramble key"), and

on said recording medium, N-pieces of encrypted content keys generated by encrypting the content key using the N-pieces of media keys are recorded (page 2, lines 56-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt and decrypt the content using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 22, Lotspiech et al. teaches the reproduction apparatus according to claim 20, but does not specifically teach wherein the encrypted content is generated by encrypting the content using a content key, on the recording medium, an encrypted content key generated by encrypting the content key using the media key is recorded,

and said reproduction apparatus is operable (a) to read out the encrypted content key from the recording medium, (b) to obtain the content key by decrypting the encrypted content key using the media key, and (c) to decrypt the encrypted content using the obtained content key.

However Masuda et al. teaches wherein the encrypted content is generated by encrypting the content using a content key (page 2, lines 49-50, the "scramble key"), on the recording medium, an encrypted content key generated by encrypting the content key using the media key is recorded (page 2, lines 53-58 and page 3, line 11, where the “second key” is the media key), and said reproduction apparatus is operable (a) to read out the encrypted content key from the recording medium (page 2, line 58 to page 3, line 2), (b) to obtain the content key by decrypting the encrypted content key using the media key (page 3, lines 3-5), and (c) to decrypt the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt and decrypt the content using an additional key as in Masuda et al. because it provides an additional layer of security.

As to claim 23, Lotspiech et al. teaches the reproduction apparatus according to claim 19,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data

held by the reproduction apparatuses of the corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each of the N-pieces), but does not specifically teach wherein

the encrypted content is generated by encrypting the content using a content key,

on the recording medium, N-pieces of encrypted content keys generated by encrypting the content key using the N-pieces of media keys are recorded, or

said reproduction apparatus is operable (a) to read out, from the recording medium, the encrypted media key data for the corresponding category, the encrypted content key for the corresponding category, and the encrypted content, (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key, (c) to obtain the content key by decrypting the encrypted content key using the obtained media key for the corresponding category, and (d) to decrypt the encrypted content using the obtained content key.

However Masuda et al. teaches wherein the encrypted content is generated by encrypting the content using a content key (page 2, lines 49-50, the "scramble key"),

on the recording medium, N-pieces of encrypted content keys generated by encrypting the content key using the N-pieces of media keys (page 2, lines 53-56 and page 3, line 11, where the “second key” is the session key block (i.e. media key) as recited in Lotspiech et al.) are recorded (page 2, lines 56-58), and

said reproduction apparatus is operable (a) to read out, from the recording medium, the encrypted media key data for the corresponding category, the encrypted content key for the corresponding category, and the encrypted content (page 2, line 58 to page 3, line 2), (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key (Lotspiech et al., column 2, lines 30-38), (c) to obtain the content key by decrypting the encrypted content key using the obtained media key for the corresponding category (page 3, lines 3-5), and (d) to decrypt the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech et al. to encrypt and decrypt the content using an additional key as in Masuda et al. because it provides an additional layer of security.

Conclusion

16. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

U.S. Patent Application Pub. No. US 2003/0142826 A1 (Asano)

U.S. Patent No. 6,609,116 (Lotspiech)

International Patent Application Pub. No. WO 02/060116 A2 (Lotspiech et al.)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRAVIS POGMORE whose telephone number is (571)270-7313. The examiner can normally be reached on Monday through Thursday between 7:30 a.m. and 5:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on 571-272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148

/T. P./
Examiner, Art Unit 4148